



# Quantum Cryptography for Long-Term Data Security

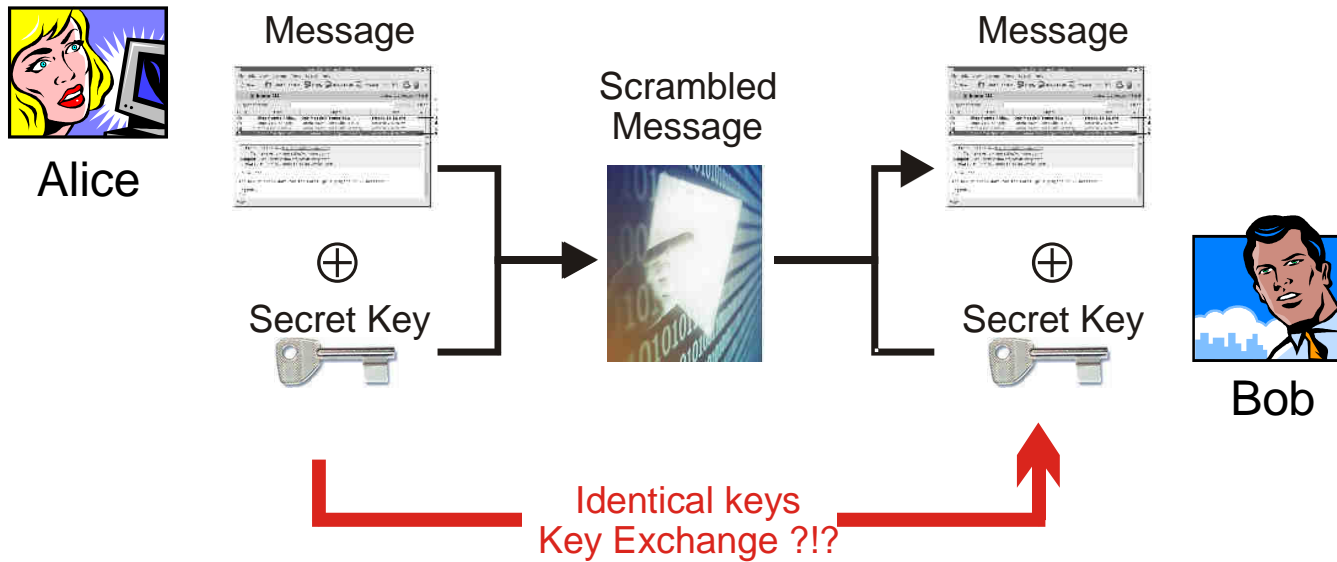
Grégoire Ribordy



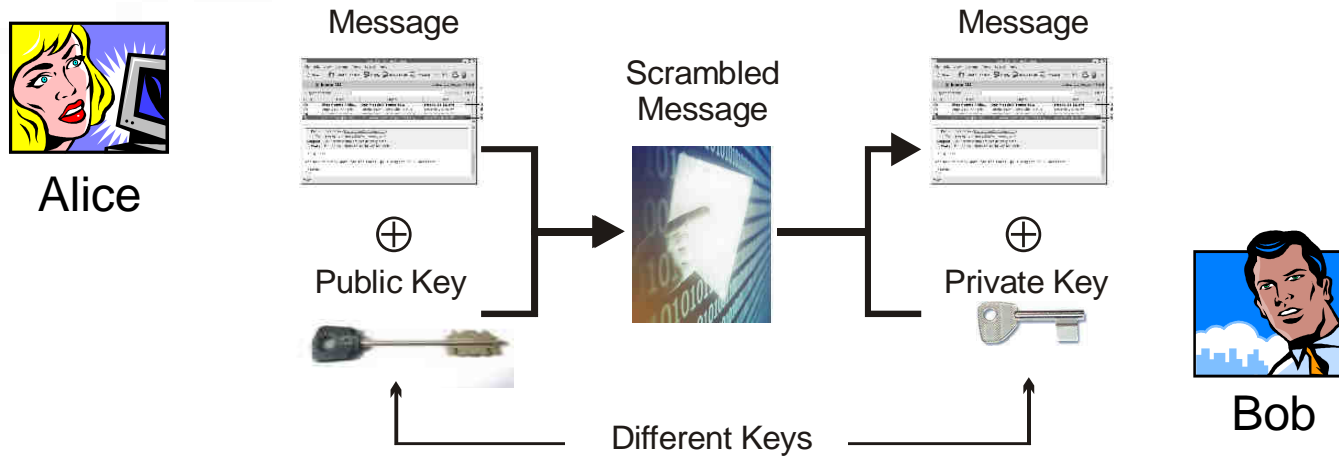
EU-Japan Collaboration Forum  
Tokyo, March 2008



# Secret Key Cryptography



# Public Key Cryptography



- Use mathematical « one-way » functions

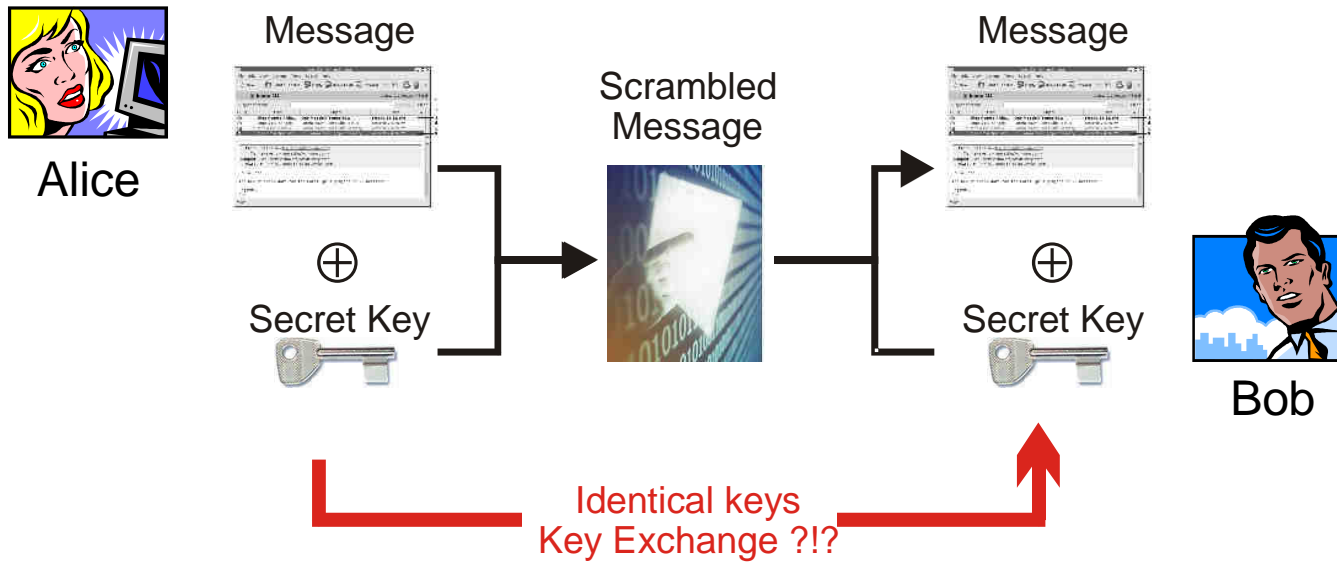
$$2'357 \times 4'201 = ?$$

$$A \times B = 9'901'757$$

- Vulnerabilities

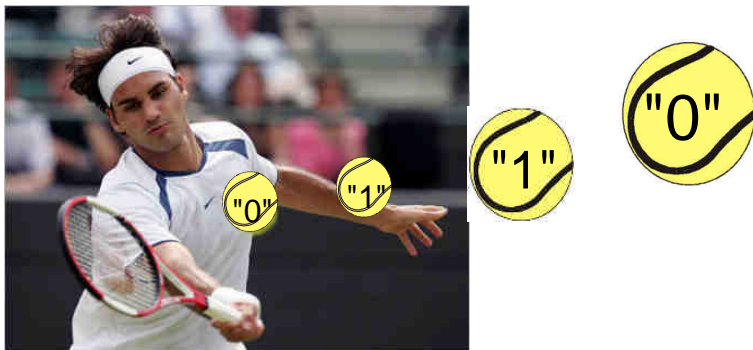
- No proof exists that « one-way » functions are « one-way »
- Computational security → Moore's law
- Quantum computing

# Secret Key Cryptography

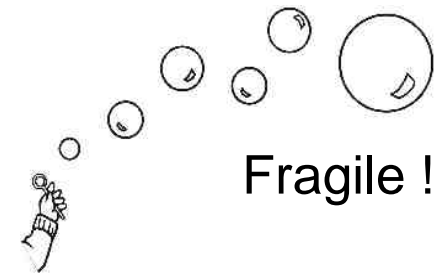


# Classical vs Quantum Communications

## Classical communication

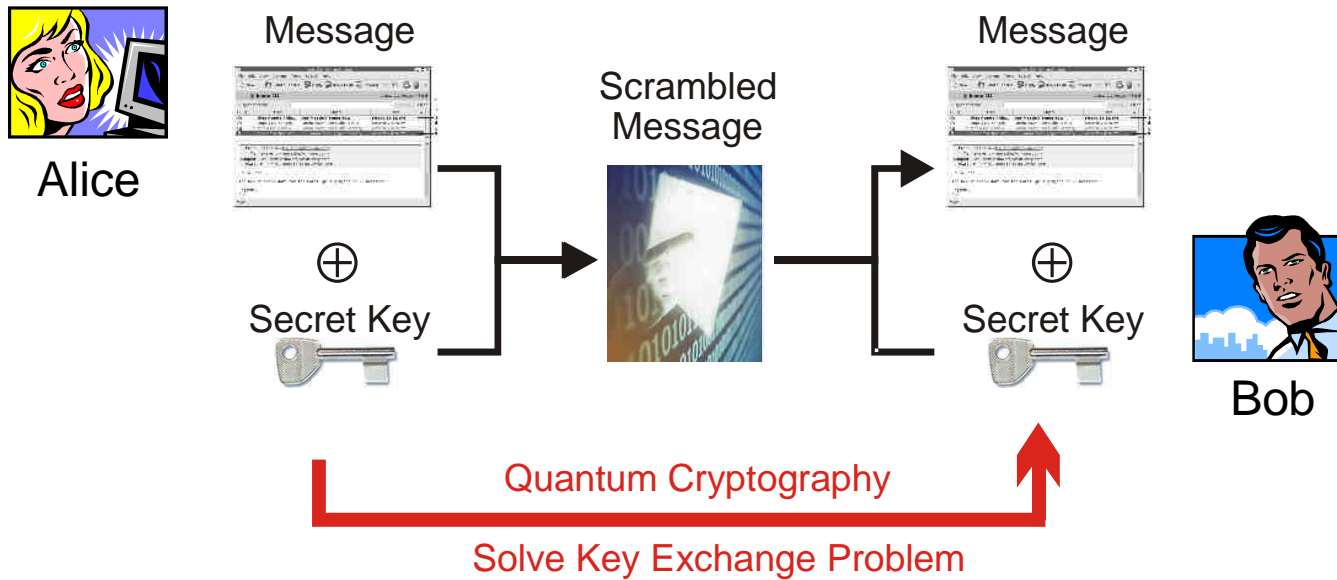


## Quantum communication



Absolute security guaranteed by the laws of quantum physics

# Solving the key exchange problem

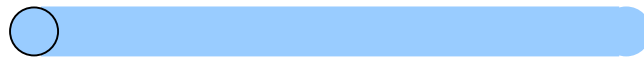


# Implementing a Quantum Cryptography Channel

➤ Necessary components



Single-Photon Source  
and Encoder



Channel



Single-Photon Decoder  
and Detector

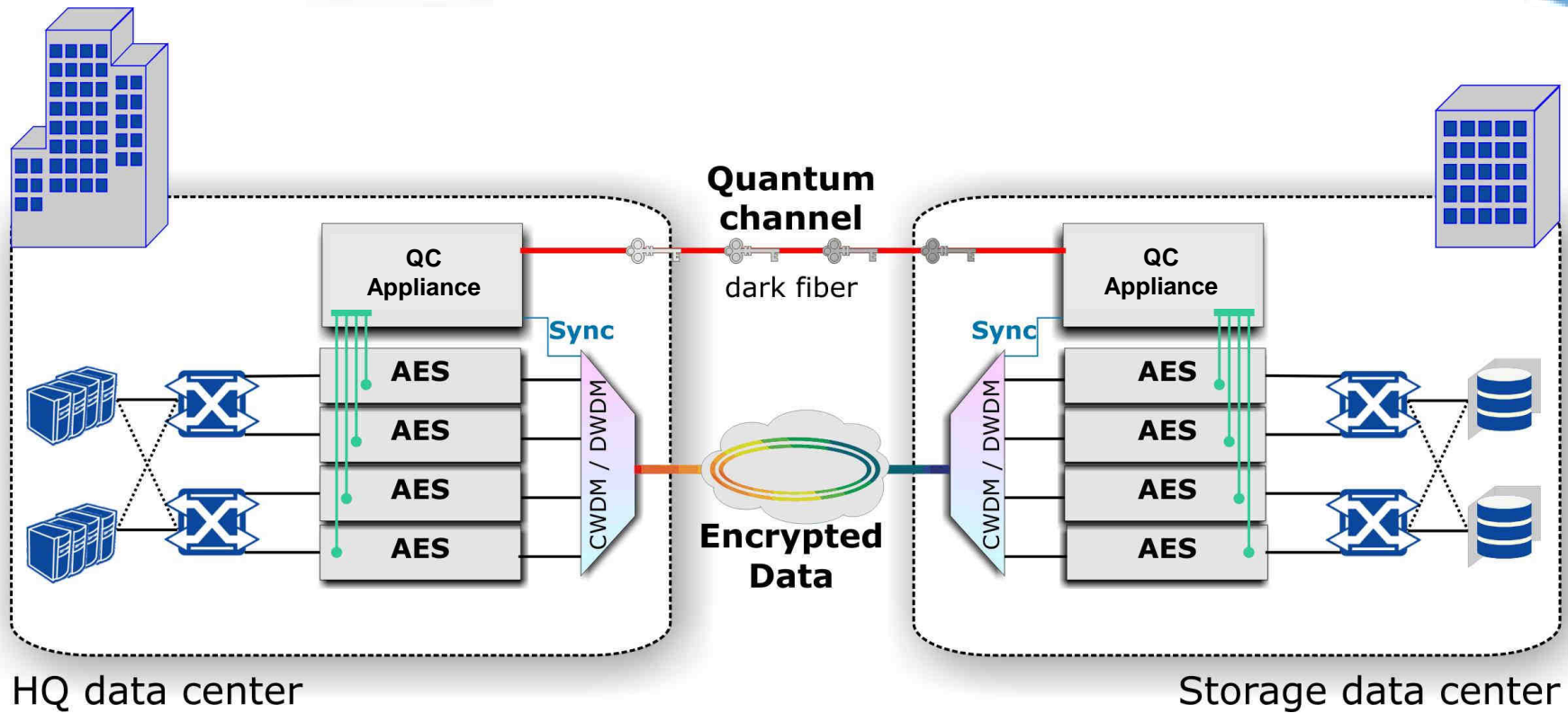
# Practical Quantum Cryptography Solution



**High-Speed Encryption Appliance**

**Quantum Cryptography Appliance**

# Quantum Cryptography Deployment Scenario



# Practical Quantum Cryptography Solution



High-Speed Encryption Appliance

Quantum Cryptography Appliance

## Main Features

- **Point-to-point** wire speed layer 2 encryption
- Encryption: AES (128, 192, 256 bits)
- Key exchange rate: QKD several keys / sec
- **Distance < 100 km (60 miles)**
- Dark fiber

Commercial Solution also available from:



US based Start-up

Advanced Prototypes developed by:

- **NEC**
- **NTT**
- **MITSUBISHI ELECTRIC**

And others...



# First Quantum Cryptography Application



REPUBLIQUE ET CANTON DE GENEVE  
Chancellerie d'Etat  
Service communication et information

Press release of Geneva State Chancellery

Geneva, October 11<sup>th</sup> 2007

## ***Geneva is counting on Quantum Cryptography as it counts its Votes***

The Swiss national elections on October 21 will mark a world first for Geneva as the canton employs quantum cryptography to protect the dedicated line used for counting its ballots. This unbreakable data code was conceived by the University of Geneva and developed industrially by its spin-off, *id Quantique*. With this

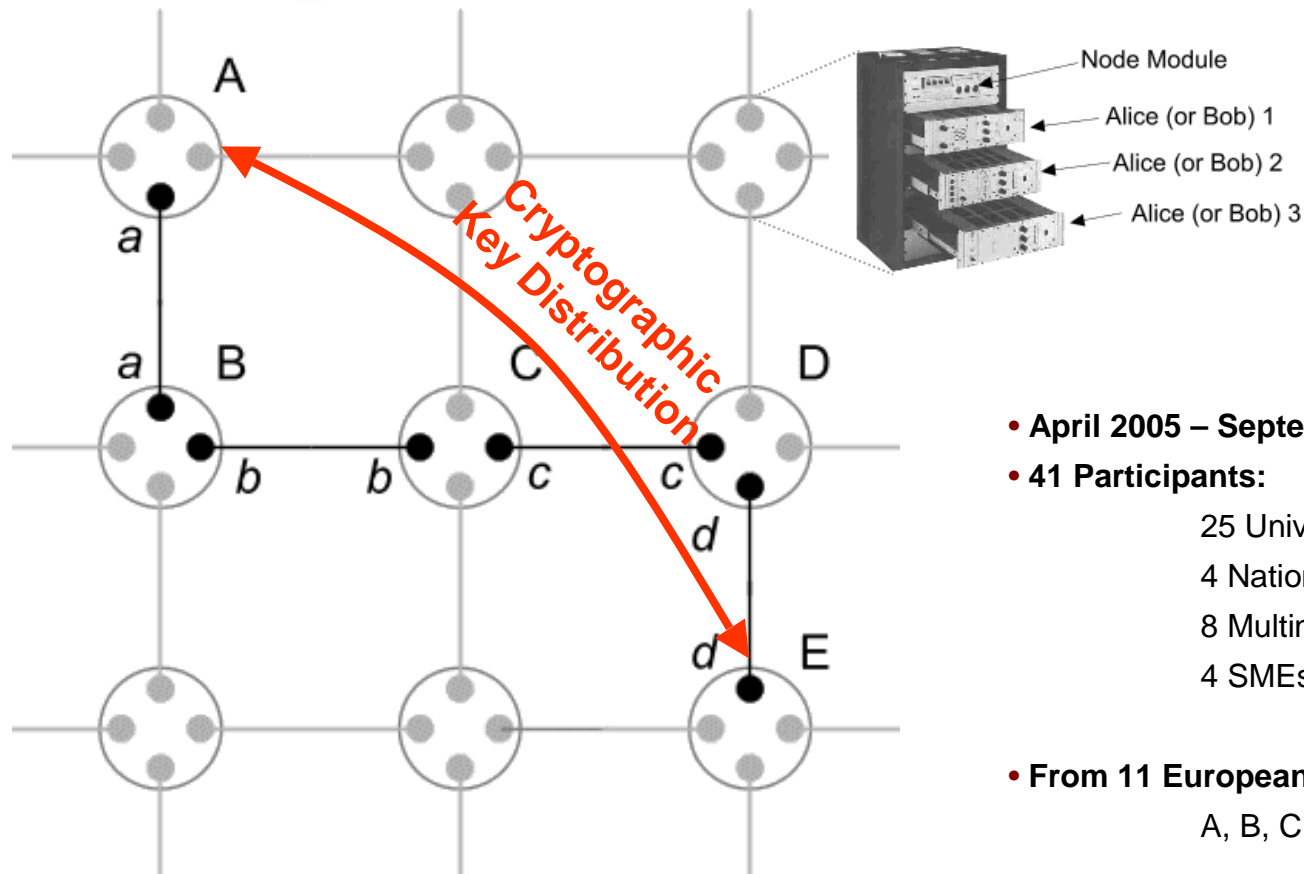
Full press release available on: [www.swissquantum.unige.ch](http://www.swissquantum.unige.ch)



# Quantum Networks

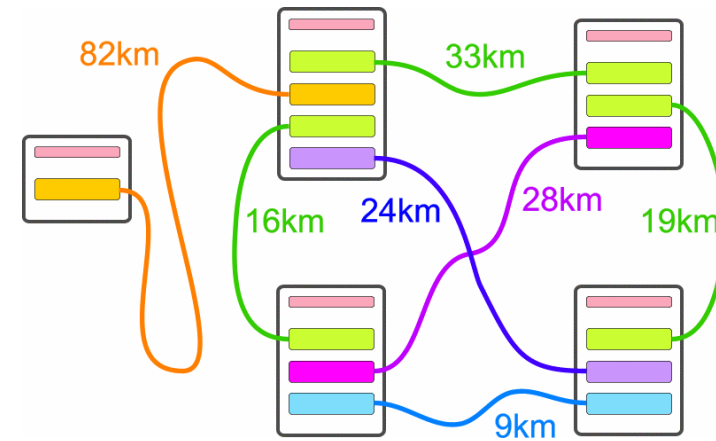


Development of a Global Network for Secure Communication based on Quantum Cryptography  
www.secoqc.net



- **April 2005 – September 2008**
- **41 Participants:**
  - 25 Universities
  - 4 National Research Centers
  - 8 Multinational Enterprises
  - 4 SMEs
- **From 11 European Countries**  
A, B, CH, CZ, D, DK, F, I, RU, S, UK
- **Funding:** 11,3 million Euros

# SECOQC Quantum Network Demonstrator

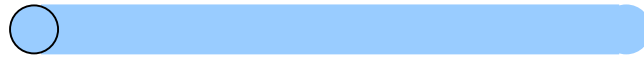


## Vienna, September 2008

- 5 QKD Technologies
- 5 Nodes / 7 Links



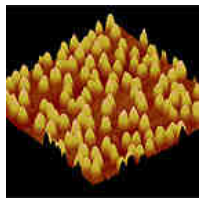
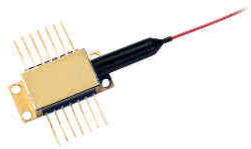
# Dedicated Components



Channel



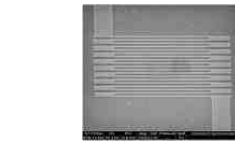
Single-Photon Source



Encoder



Decoder



Single-Photon Detector

# International Collaboration Required

- Today: Standards for Quantum Cryptography don't exist
- Standards are extremely important for the commercial development of quantum cryptography
  - Possibility to compare products
  - Possibility to certify products
  - ...
- Efforts have been initiated
  - Standardization work started at ETSI in January 2008
  - Telcordia workshop in the US on March 3rd
- International collaboration is essential for meaningful standard development



Thank you for your attention

Grégoire Ribordy  
gregoire.ribordy@idquantique.com

id Quantique SA  
Ch. Marbrerie 3  
CH – 1227 Carouge  
Phone: +41 (0)22 301 83 71

[www.idquantique.com](http://www.idquantique.com)

## Support

---

EU FP6



Switzerland

